(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 09034822 A

(43) Date of publication of application: 07.02.97

(51) Int. Cl G06F 13/00
G06F 15/00

(21) Application number: 07183907

(22) Date of filing: 20.07.95

(71) Applicant: FUJI XEROX CO LTD

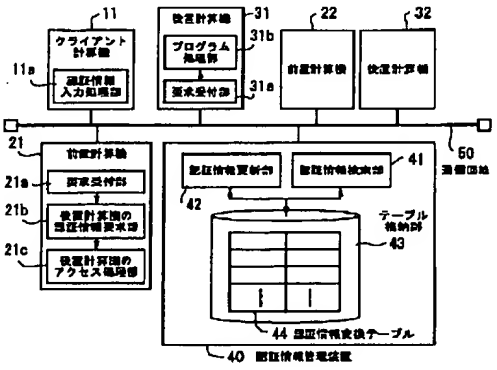
(72) Inventor: YAMAUCHI HIROSHI

(54) VERIFICATION INFORMATION MANAGEMENT EQUIPMENT

(57) Abstract:

PROBLEM TO BE SOLVED: To eliminate the need for input of each verification information in the case of access to a post-stage computer being other server computer from a client computer via a pre-stage computer being a server computer.

SOLUTION: A verification information management equipment 40 conducts altogether the management of verification information having been conducted by each server computer. The equipment has a table storage section 43 storing a verification information conversion table 44 for a post-computer and verification information of each server computer. Furthermore, the equipment has a verification information retrieval section 41 that retrieves the verification information conversion table 44 in response to a request from the pre-stage computer to read verification information out of the post-stage computer 21 and sends the information to the pre-stage computer requesting the transmission of information. Moreover, the equipment has a verification information update section 42 that registers the verification information given by a client computer to the verification information conversion table 44 when the client computer has not made user registration.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開平9－34822

(43)公開日　平成９年(1997)２月７日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ	13/00	３５７	9460－5E	Ｇ０６Ｆ	13/00	３５７Ｚ
	15/00	３３０	9364－5L		15/00	３３０Ａ

審査請求　未請求　請求項の数１　ＯＬ　（全 ９ 頁）

(21)出願番号　特願平7－183907

(22)出願日　平成７年(1995)７月20日

(71)出願人　000005496
富士ゼロックス株式会社
東京都港区赤坂二丁目17番22号

(72)発明者　山内　博史
神奈川県川崎市高津区坂戸３丁目２番１号
ＫＳＰ　Ｒ&Ｄビジネスパークビル　富士ゼロックス株式会社内

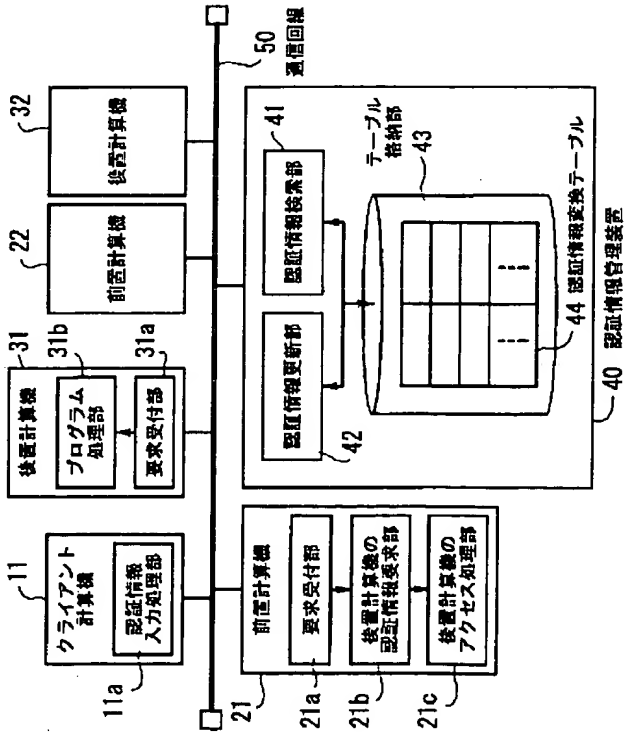
(74)代理人　弁理士　服部　毅巖

(54)【発明の名称】　認証情報管理装置

(57)【要約】

【目的】　クライアント計算機からあるサーバ計算機である前置計算機２１を介した別のサーバ計算機である後置計算機３１へのアクセス時に、それぞれの認証情報の入力の必要がないようにする。

【構成】　サーバ計算機が個々に行っていた認証情報の管理を認証情報管理装置４０が一括して行う。この装置は、各サーバ計算機の認証情報および後置計算機用の認証情報変換テーブル４４を格納するテーブル格納部４３を有する。また、認証情報検索部４１を有し、前置計算機からの要求に応じて認証情報変換テーブル４４を検索して後置計算機の認証情報を読み出し、要求した前置計算機へ送信する。前置計算機２１はその認証情報で後置計算機３１にアクセスする。さらに、認証情報更新部４２を有し、利用者登録がない場合にクライアント計算機によって与えられた認証情報を認証情報変換テーブル４４に登録する。



1

【特許請求の範囲】

【請求項１】　クライアント計算機と、クライアント計算機から直接アクセスされる前置計算機と、クライアント計算機から前記前置計算機を介して間接的にアクセスされる後置計算機とがネットワークで接続された計算機システムにて、認証情報を管理する認証情報管理装置であって、

前記後置計算機毎にユーザに対応した認証情報を記憶する記憶手段と、

前記前置計算機のアクセス後に当該前置計算機を介して間接的に後置計算機をアクセスする際に受け取る当該後置計算機の識別情報とユーザー情報とを基に前記記憶手段から該当する後置計算機の認証情報を検索する検索手段と、

前記検索手段で検索された認証情報を当該前置計算機に返信する通信手段と、

を具備することを特徴とする認証情報管理装置。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は認証情報管理装置に関し、特に疎結合された計算機システムにおける異機種間の利用者認証情報を一括して管理する認証情報管理装置に関する。

【０００２】

【従来の技術】複数の計算機をネットワークによって相互に接続し、ネットワーク上の情報や資源を共用するクライアント・サーバ型のシステムが一般的になってきている。ここで、利用者がクライアント計算機からサーバ計算機にアクセスする場合に、利用者認証情報を使用してその利用者が利用を許可された当人であることを認証することが行われている。同様に、利用者がクライアント計算機からあるサーバ計算機（以下、前置計算機という）を介して別のサーバ計算機（以下、後置計算機という）にアクセスする場合にも、通常、サーバ計算機はそれぞれ認証方式が異なるので、それぞれ利用者認証情報を使用してアクセスすることになる。

【０００３】このため、利用者が前置計算機を介して後置計算機にアクセスする場合には、利用者は前置計算機と後置計算機とで２回、認証情報の入力を要求されることになる。これに対し、従来より、前置計算機を介して後置計算機にアクセスがあった場合に、後置計算機であることを利用者が意識することなく、後置計算機のサービスを利用できるようにする認証方式が知られている。

【０００４】たとえば、特開平４－７１０５８号公報に記載の計算機システムでは、前置計算機と後置計算機とから構成されており、前置計算機および後置計算機は、通信回線によって疎結合されている。そして、それぞれの計算機は、異なった認証情報を必要としているとする。このシステムを利用する端末から前置計算機を介して後置計算機にアクセスする場合、利用者は、後置計算機にアクセスするために認証情報を入力しなくてはならない。そこで、この計算機システムでは、前置計算機の中にあらかじめ後置計算機の認証に必要な情報を登録しておき、利用者が後置計算機にアクセスする時、自動的に前置計算機が登録された情報を後置計算機に送ることで、利用者が後置計算機にアクセスする際に生じる利用者認証情報入力処理の問題を解決している。

2

【０００５】また、特開平６－２７４４３１号公報に記載の異機種接続環境における認証および認可方式によれば、異機種接続環境でのクライアント・サーバ型のシステムにおいて、クライアントからサーバへのアクセスの認証を行う方法として、ケルベロスと呼ばれる認証方式がある。ケルベロスは、セキュリティサーバという計算機を持ち、この計算機では、ネットワークに一意なユーザ識別子を持っている。ところが、セキュリティサーバの持つユーザ識別子は、サーバが持つユーザ識別子と異なる。また、ファイルへのアクセスの認可の権限を決める属性値は、サーバが持つユーザ識別子に依存する。そのため、セキュリティサーバを用いてファイルにアクセスする場合、ファイルにアクセスするたびにサーバ固有のユーザ識別子を入力しなければならない。そこで、この認証および認可方式では、サーバ内に、セキュリティサーバの持つユーザ識別子をサーバが持つユーザ識別子に変換する機構を設けることで、ユーザ識別子を入力することなくサーバ内のファイルにアクセスすることができるようにしている。

【０００６】

【発明が解決しようとする課題】クライアント・サーバ型の計算機システムで、サーバ計算機が前置計算機と後置計算機に分散させているシステムにおいて、クライアントから前置計算機（またはセキュリティサーバ）を介して後置計算機にアクセスする場合、利用者は、後置計算機にアクセスする度にユーザ識別子を入力しなければならないという問題を、上記したいずれの従来例も、前置計算機内にユーザ識別子変換機構を設けることによって、解決している。

【０００７】ところが、前置計算機が複数存在し、かつそれらの前置計算機が同じ後置計算機をアクセスする場合、上記の従来例の認証方式では、その後置計算機の認証情報が変わったときには、その後置計算機をアクセスする前置計算機毎にユーザ識別子変換機構の認証情報を更新しなければならないという問題点があった。

【０００８】本発明はこのような点に鑑みてなされたものであり、クライアント計算機から前置計算機を介して後置計算機をアクセスする際に個々に認証情報を入力する必要がなく、利用者は、サーバ計算機が前置計算機と後置計算機とに分かれていることを意識することなく、後置計算機にアクセスすることができる認証情報管理装置を提供することを目的とする。

【０００９】また、本発明は後置計算機の認証情報が変

わっても、これをアクセスする前置計算機において個々に認証情報を更新する必要がない認証情報管理装置を提供することを目的とする。

【００１０】

【課題を解決するための手段】本発明では上記課題を解決するために、クライアント計算機と、クライアント計算機から直接アクセスされる前置計算機と、クライアント計算機から前置計算機を介して間接的にアクセスされる後置計算機とがネットワークによって接続された計算機システムにおいて、サーバ計算機が個々に行っていた認証情報の管理を専用の認証情報管理装置（図１の４０）で行うようにする。この認証情報管理装置は、後置計算機毎にユーザに対応した認証情報を記憶する記憶手段（４３）と、前置計算機のアクセス後に当該前置計算機を介して間接的に後置計算機をアクセスする際に受け取る当該後置計算機の識別情報とユーザ情報とを基に記憶手段から該当する後置計算機の認証情報を検索する検索手段（４１）と、この検索手段で検索された認証情報を当該前置計算機へ返信する通信手段（４１）とを具備している。

【００１１】好ましくは、さらに、入力装置またはクライアント計算機からの入力情報に基づいて、記憶手段に認証情報を設定する設定手段（４２）とを具備している。

【００１２】

【作用】上述の手段によれば、クライアント計算機から前置計算機へアクセスする場合には、クライアント計算機は認証情報管理装置に照会し、通常の認証方式にて認証されることで前置計算機へのアクセスが可能になる。その後、クライアント計算機が前置計算機に対して後置計算機へのアクセス要求を出すと、前置計算機は認証情報管理装置にアクセスしたい後置計算機のサーバ情報を送信する。ここで、サーバ情報としては、後置計算機の識別情報と前置計算機がクライアント計算機を認証したときのユーザ情報とを通知する。認証情報管理装置では、検索手段がその後置計算機の識別情報およびユーザ情報をキーにして記憶手段に記憶されている後置計算機の認証情報を検索し、通信手段を通じて前置計算機へ送信する。前置計算機は得られた認証情報を基にして後置計算機へアクセスする。すなわち、前置計算機がその認証情報を以て認証情報管理装置に照会し、通常の認証方式にて認証されることにより後置計算機へのアクセスが可能になる。なお、検索手段による認証情報の検索にて、記憶手段の認証情報に後置計算機についての利用者登録がなされていない場合、または後置計算機へのアクセスが認証情報の変更などで認証されなかった場合には、クライアント計算機に対し認証情報入力要求を出し、クライアント計算機は認証情報を入力して認証情報管理装置に認証情報登録・更新要求を出す。認証情報管理装置では、設定手段が入力された認証情報に従って記憶手段に登録または該当する情報を更新する。

【００１３】

【実施例】以下、本発明の実施例を添付図面を参照して説明する。図１は本発明の認証情報管理装置を含む計算機システムのネットワーク構成例を示す図である。

【００１４】図示の計算機システムは、クライアント計算機１１と、サーバ計算機である前置計算機２１，２２および後置計算機３１，３２と、認証情報管理装置４０とからなる。それぞれの計算機は、通信回線５０によって接続されている。なお、実際の計算機システムでは、多数のクライアント計算機およびサーバ計算機が通信回線５０によって接続されている。認証情報管理装置４０は認証情報検索部４１と、認証情報更新部４２と、認証情報変換テーブル４４を格納するテーブル格納部４３とから構成されている。

【００１５】ここで、クライアント計算機１１から前置計算機２１を経由して後置計算機３１にアクセスし、後置計算機３１のアプリケーションプログラムを実行する場合を例にして説明する。したがって、この例の実行のために、前置計算機２１は要求受付部２１ａと、後置計算機の認証情報要求部２１ｂと、後置計算機のアクセス処理部２１ｃとを有し、後置計算機３１は要求受付部３１ａと、プログラム処理部３１ｂとを有している。また、クライアント計算機１１は認証情報を登録するための認証情報入力処理部１１ａを有している。そして、認証情報管理装置４０はどのサーバ計算機からもブロードキャストによって、サーバ名を指定しなくてもアクセスすることができるものとする。

【００１６】認証情報は、クライアント計算機１１の認証情報入力処理部１１ａより認証情報管理装置４０にアクセスし、その認証情報更新部４２によってテーブル格納部４３の認証情報変換テーブル４４に利用したいサーバ計算機の情報とともに登録されている。この例では、利用者は少なくとも後置計算機３１について認証情報変換テーブル４４に登録されている。

【００１７】まず、クライアント計算機１１から前置計算機２１へアクセスする場合には、クライアント計算機１１は認証情報を認証情報管理装置４０に送信する。認証情報管理装置４０では、テーブル格納部４３に格納された図示しない認証情報テーブルを利用して、通常の認証方式で前置計算機２１へのアクセスを認証する。

【００１８】前置計算機２１へのアクセスの後、クライアント計算機１１からの要求に後置計算機３１へアクセスしてその中のアプリケーションプログラムを実行する要求が含まれていたとすると、前置計算機２１の要求受付部２１ａはその後置計算機３１へのアクセス要求を受け付け、後置計算機の認証情報要求部２１ｂは認証情報管理装置４０に前置計算機２１がクライアント計算機１１を認証したときのユーザ識別子および後置計算機３１のサーバ識別子とともに認証情報検索要求を送信する。

認証情報管理装置４０ではこの要求を受けて、認証情報検索部４１が認証情報変換テーブル４４をユーザ識別子およびサーバ識別子をキーにして検索し、後置計算機３１へアクセスするのに必要な認証情報を読み出し、前置計算機２１へ送信する。前置計算機２１では、その後置計算機のアクセス処理部２１ｃにより、認証情報管理装置４０から受けた認証情報を以て後置計算機３１へアクセスする。すなわち、その認証情報を認証情報管理装置４０に送信し、通常の認証方式にて後置計算機３１へのアクセスを認証する。後置計算機３１では、要求受付部３１ａにおいて、クライアント計算機１１からのアプリケーションプログラム実行要求を受け付け、プログラム処理部３１ｂによりアプリケーションプログラムを実行することになる。

【００１９】図２は本発明の認証情報管理装置の構成例を示すブロック図である。認証情報管理装置４０において、その認証情報検索部４１は認証情報の検索要求を受け付けたり、検索した認証情報を要求した前置計算機へ返送する認証情報検索受付部４１ａと、テーブル格納部４３の認証情報変換テーブル４４に対して検索要求のあった認証情報の検索を実行する認証情報検索部４１ｂと、検索の結果から要求された認証情報が登録されているかどうかを判定する判定部４１ｃと、認証情報変換テーブル４４から認証情報を読み出す認証情報読み出し部４１ｄとによって構成されている。また、認証情報更新部４２は利用者からの認証情報の登録・更新要求を受け付ける認証情報登録受付部４２ａと、認証情報変換テーブル４４に対して認証情報の登録・更新処理を実行する認証情報変換テーブル更新処理部４２ｂとによって構成されている。

【００２０】前置計算機から後置計算機へアクセスするための認証情報の取得要求があると、その要求は認証情報検索部４１の認証情報検索受付部４１ａにて受け付け、認証情報検索部４１ｂがテーブル格納部４３の認証情報変換テーブル４４を検索する。ここで、判定部４１ｃが認証情報の登録・未登録を判定し、登録済みであれば、認証情報読み出し部４１ｄが認証情報変換テーブル４４から認証情報を読み出して要求元の前置計算機に送信し、未登録であれば、クライアント計算機に対して認証情報入力要求を送信する。クライアント計算機において認証情報が入力され、認証情報管理装置４０に認証情報登録要求が送信されると、この要求は認証情報登録受付部４２ａが受け付け、認証情報変換テーブル更新処理部４２ｂが認証情報変換テーブル４４に認証情報の登録を行う。

【００２１】また、後置計算機へのアクセス時の認証が失敗したときには、その後置計算機の認証情報は変更されていることになる。この場合にも、クライアント計算機に対して認証情報の入力要求を出す。これに応じてクライアント計算機で認証情報が入力され、更新要求とともに認証情報更新部４２の認証情報登録受付部４２ａにて受け付けられ、認証情報変換テーブル更新処理部４２ｂによって該当する認証情報の更新が行われる。

【００２２】図３は認証情報変換テーブルの一例を示す図である。認証情報変換テーブル４４は、図示のように、サーバ識別子・ユーザ識別子と認証情報との対応テーブルになっている。サーバ識別子・ユーザ識別子のフィールドには、サーバ計算機の名前および利用者の名前を表す識別子が入力され、認証情報のフィールドには、たとえば利用者の名前を表すユーザ識別子およびパスワードが入力される。したがって、認証情報検索部４１ｂがこの認証情報変換テーブル４４を検索する場合には、サーバ識別子およびユーザ識別子をキーにして検索が行われることになる。

【００２３】次に、クライアント計算機から前置計算機を介した後置計算機へのアクセスの場合に処理の流れについて説明する。図４は後置計算機へのアクセス処理の内容を示すフローチャートである。

【００２４】クライアント計算機１１から前置計算機２１を介した後置計算機３１へのアクセスの場合は、まず、前置計算機２１へのアクセスから始まる。すなわち、クライアント計算機１１は、認証情報管理装置４０にたとえばユーザ識別子およびパスワードを含む認証情報を送り、前置計算機２１へのアクセスの認証を得る。

【００２５】ここで、クライアント計算機１１から前置計算機２１に対して後置計算機３１へのアクセス要求があると（ステップＳ１）、前置計算機２１は、認証情報管理装置４０に対して、アクセスしたい後置計算機３１のサーバ識別子と前置計算機２１のクライアント計算機１１を認証したときのユーザ識別子とを送る（ステップＳ２）。

【００２６】一方、認証情報管理装置４０では、送られきたサーバ識別子・ユーザ識別子をキーにして、認証情報検索部４１ｂがテーブル格納部４３に格納されている認証情報変換テーブル４４を検索し、判定部４１ｃにて後置計算機３１の認証情報が登録済みかどうかを判定する（ステップＳ３）。後置計算機３１の認証情報が登録済みであれば、認証情報読み出し部４１ｄが認証情報変換テーブル４４から該当する後置計算機３１の認証情報を読み出し（ステップＳ４）、読み出した後置計算機３１の認証情報を前置計算機に送信する（ステップＳ５）。

【００２７】ステップＳ３の判定において、後置計算機３１の認証情報が未登録であれば、認証情報を新たに登録しなければならないので、後述の認証情報更新処理に進む（ステップＳ６）。

【００２８】そして、前置計算機２１では、認証情報管理装置４０から受けた後置計算機３１の認証情報を基に後置計算機３１にアクセスする（ステップＳ７）。すなわち、前置計算機２１は受けた認証情報を認証情報管理

7

装置４０に送信し、通常の認証方式にて後置計算機３１へのアクセスを認証する。その後は、後置計算機３１での処理になる。

【００２９】次に、後置計算機３１の認証情報が未登録または変更の場合の認証情報の登録・更新処理について説明する。図５は認証情報登録処理の内容を示すフローチャートである。

【００３０】認証情報管理装置４０の認証情報検索部４１における判定部４１ｃにおいて、後置計算機３１の認証情報が登録されていないとの判定があった場合には、認証情報管理装置４０はクライアント計算機１１に対して後置計算機３１の認証情報の入力を要求する（ステップＳ１１）。すると、クライアント計算機１１は認証情報入力処理部１１ａにより認証情報の入力処理を行い（ステップＳ１２）、入力された後置計算機３１の認証情報を認証情報管理装置４０に送信する（ステップＳ１３）。認証情報管理装置４０では、クライアント計算機１１より受けた後置計算機３１の認証情報を認証情報更新部４２によって認証情報変換テーブル４４に登録する（ステップＳ１４）。

【００３１】また、後置計算機３１へのアクセス時に後置計算機３１の認証情報が変更されていた場合には、認証情報変換テーブル４４の後置計算機３１の認証情報を変更しなければならないので、後置計算機３１のアクセス時に非認証であった場合にも、この図５のフローチャートのステップＳ１１から同様の処理を開始する。

【００３２】上述のように、認証情報を一括管理する認証情報管理装置をネットワーク上に新たに設けることにより、利用者は、後置計算機にアクセスする毎に、認証情報を入力する必要がなくなるため、利用者の労力が軽減されるだけではなく、後置計算機の認証情報が更新されても、認証情報管理装置に登録されている情報の更新だけでよいので、利用者の労力が軽減される。

【００３３】なお、ＵＮＩＸネットワークにおけるＤＮＳ（Ｄｏｍａｉｎ　Ｎａｍｅ　Ｓｅｒｖｉｃｅ）のように、ローカルエリアネットワークの同一ドメイン内で認証情報を共有している場合がある。そこで、認証情報管理装置内の情報を共有している後置計算機の認証情報を

8

同一の認証情報でアクセス可能な計算機同士をカテゴリーに分類して認証情報管理装置に登録しておくこともできる。この管理方法を採ることにより、認証情報変換テーブル４４のデータ量を少なくできるだけでなく、同一の認証情報でアクセス可能な計算機を一度に更新することができるため、認証情報の更新の際の処理を減少させることができる。

【００３４】

【発明の効果】以上説明したように本発明では、サーバ計算機以外に認証情報管理装置を設置し、ユーザが前置計算機を介して後置計算機を通じてアクセスする際に、認証情報管理装置にアクセス要求を出し、後置計算機の認証情報を得るように構成した。このため、前置計算機を介して後置計算機にアクセスする都度、後置計算機の認証情報を入力する必要がなく、後置計算機の認証情報が変更されたとき、認証情報管理装置に登録されているを認証情報を更新するだけで済む。

【図面の簡単な説明】

【図１】本発明の認証情報管理装置を含む計算機システムのネットワーク構成例を示す図である。

【図２】本発明の認証情報管理装置の構成例を示すブロック図である。

【図３】認証情報変換テーブルの一例を示す図である。

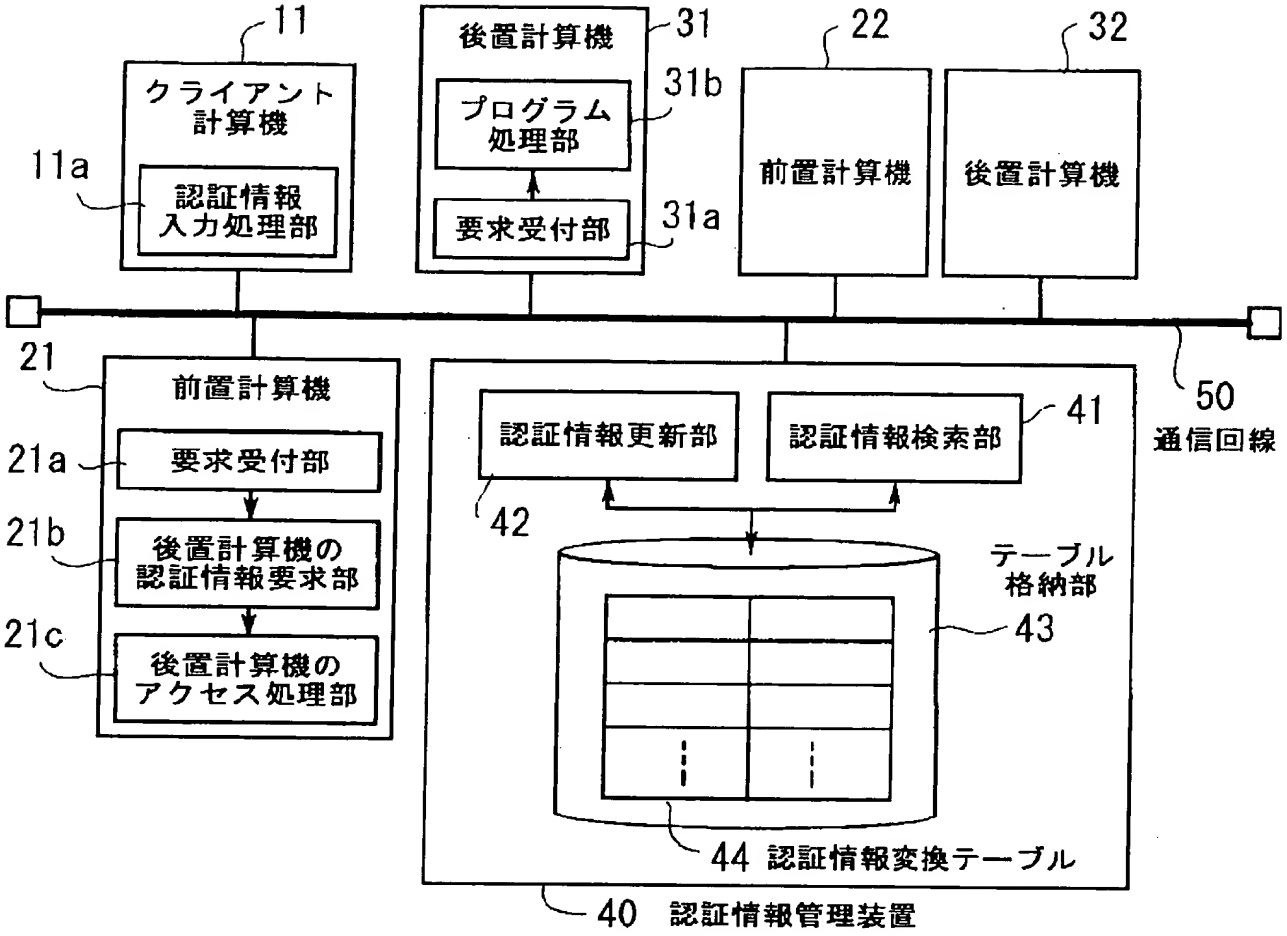
【図４】後置計算機へのアクセス処理の内容を示すフローチャートである。

【図５】認証情報登録処理の内容を示すフローチャートである。

【符号の説明】

１１　クライアント計算機
２１，２２　前置計算機
３１，３２　後置計算機
４０　認証情報管理装置
４１　認証情報検索部
４２　認証情報更新部
４３　テーブル格納部
４４　認証情報変換テーブル
５０　通信回線

【図１】

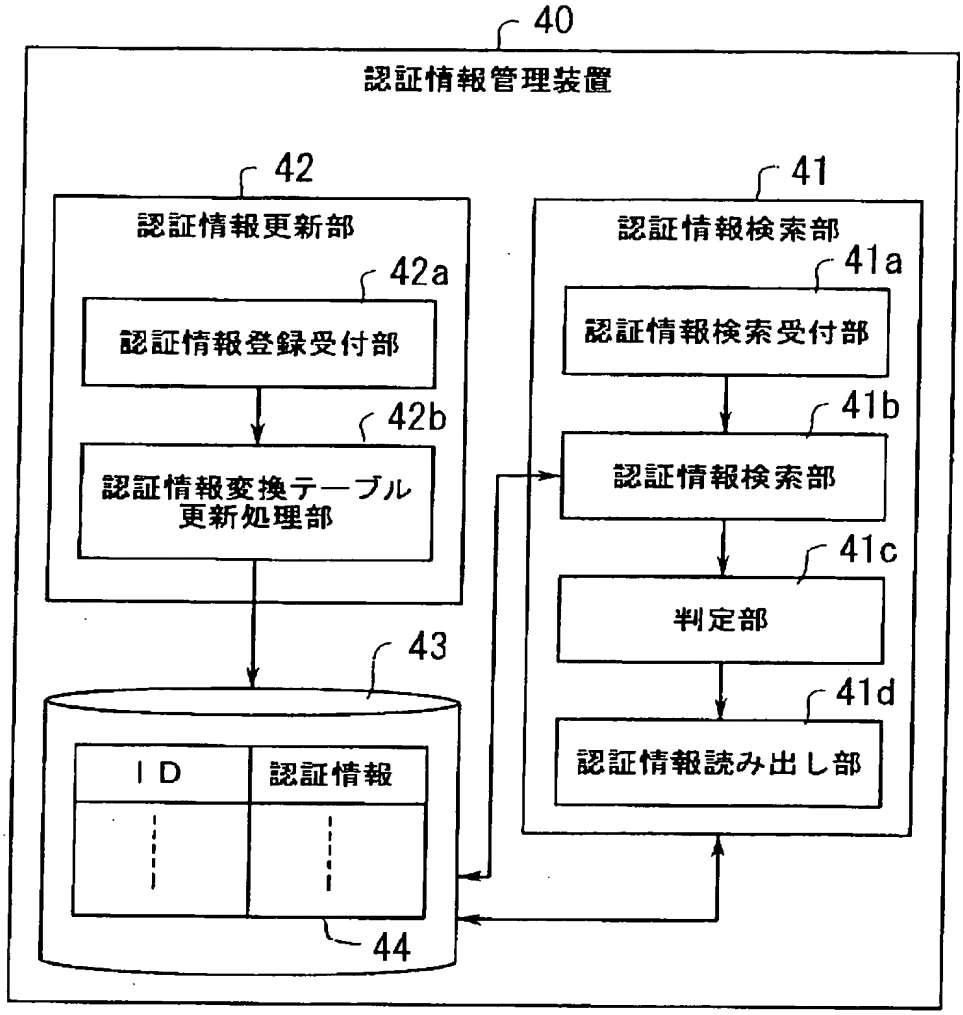


【図３】

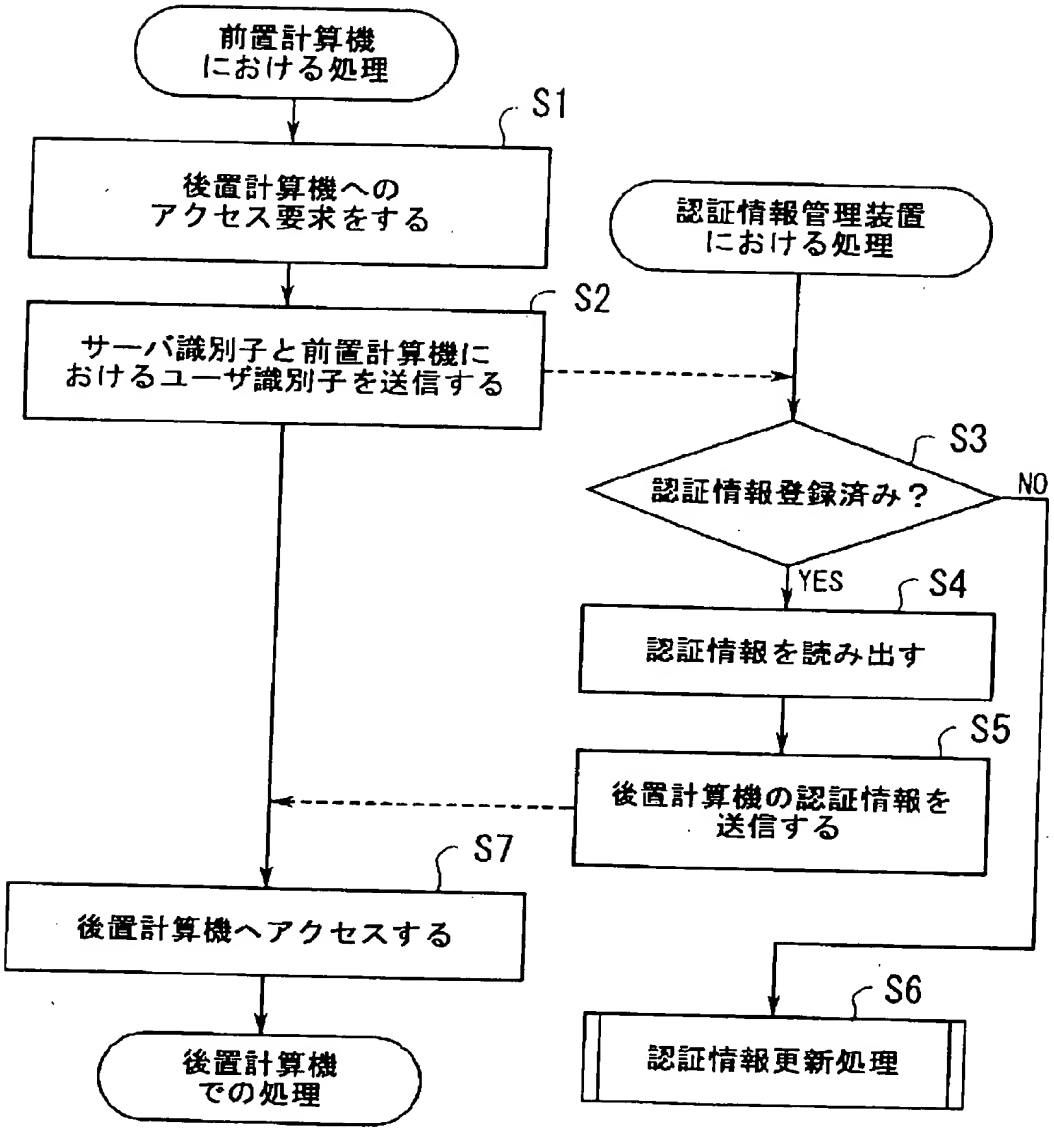
44

サーバ識別子・ユーザ識別子	認証情報
server1, username1	usernameA, password1
server1, username2	usernameB, password2
server2, username1	usernameC, password3
server3, username1	usernameD, password4
server4, username1	usernameE, password5
⋮	⋮

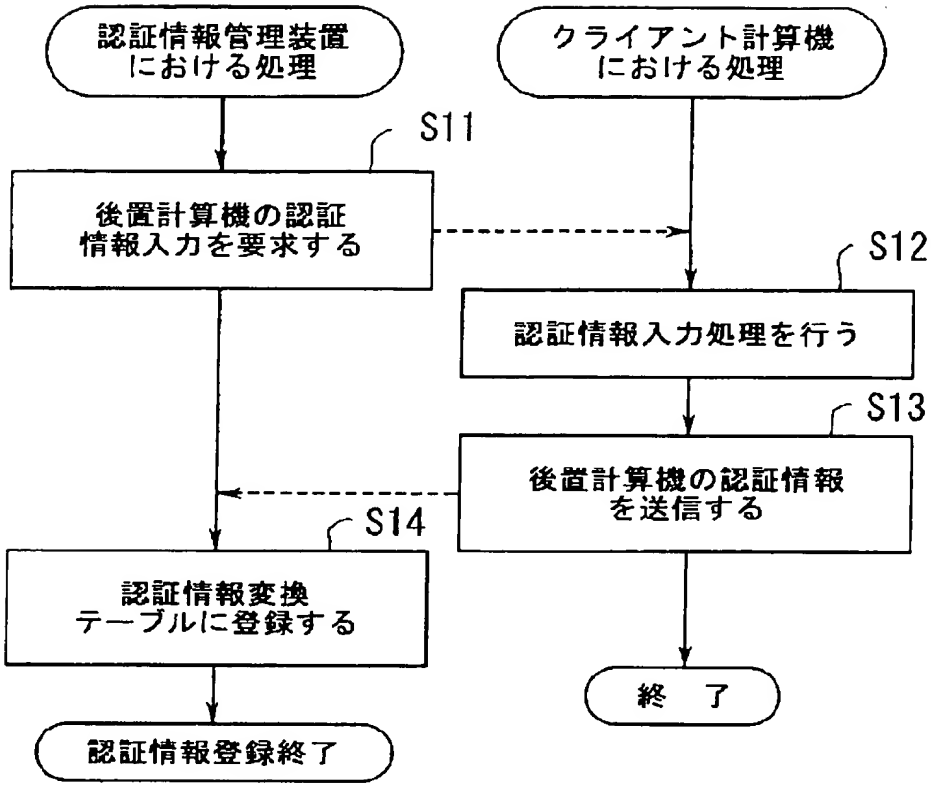
【図２】


40
認証情報管理装置
42
認証情報更新部
42a
認証情報登録受付部
42b
認証情報変換テーブル
更新処理部
43
ＩＤ
認証情報
44
41
認証情報検索部
41a
認証情報検索受付部
41b
認証情報検索部
41c
判定部
41d
認証情報読み出し部

【図４】


前置計算機
における処理
S1
後置計算機への
アクセス要求をする
認証情報管理装置
における処理
S2
サーバ識別子と前置計算機に
おけるユーザ識別子を送信する
S3
認証情報登録済み？
NO
YES
S4
認証情報を読み出す
S5
後置計算機の認証情報を
送信する
S7
後置計算機へアクセスする
S6
認証情報更新処理
後置計算機
での処理

【図５】


認証情報管理装置
における処理
クライアント計算機
における処理
S11
後置計算機の認証
情報入力を要求する
S12
認証情報入力処理を行う
S13
後置計算機の認証情報
を送信する
S14
認証情報変換
テーブルに登録する
終　了
認証情報登録終了